Аладдин РД

Задачи применения мобильных устройств для использования квалифицированной ЭП и некоторые способы их решения

Сергей Груздев
Генеральный директор

18.09.2012

О чем?

1. **Портальные решения и облачные сервисы**
   - Сервисам нужна юридическая значимость
2. **Мобильные платформы**
   - Квалифицированная ЭП для мобильных устройств
3. **Смарт-карт технологии**
   - Платежная карта с ЭП “на борту” поможет сделать эл. услуги массовыми
   - SIM-карта с ЭП
4. **Сегмент M2M**
   - Передаваемым данным надо доверять (нужна ЭП)
5. **Доверенная среда у массового пользователя?**
   - Надо менять парадигму

Развитие корпоративной мобильности

BYOD (Bring Your Own Device) —

Принеси свое собственное устройство

Gartner:

К 2014 году 90% компаний будут поддерживать корпоративные приложения на устройствах, которые находятся в собственности работников

http://www.gartner.com/resId=2004115

Gartner:

«Внедрение пользовательских устройств (смартфонов и планшетов) в корпоративные ИТ-системы будет самым значительным трендом, влияющим на ИТ в ближайшие 10 лет».

Основные отрасли — финансы и страхование, так как в них работает наибольшее количество мобильных сотрудников»

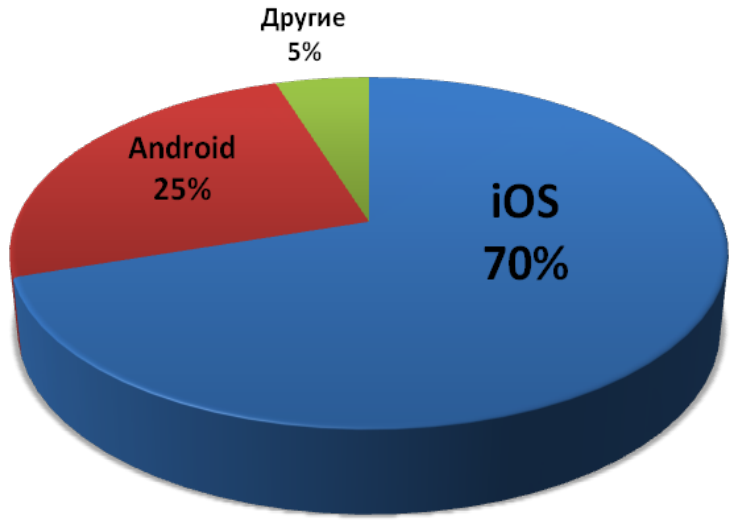
Мобильные платформы и PKI

Плюсы

- МУ всегда с собой, есть у всех (огромная инсталляционная база)

Проблемы

- Быстрая смена поколений (быстрее, чем мы успеваем разрабатывать приложения и сертифицировать свои средства)
- Множество платформ, хотя ситуация быстро меняется.
  - Для нашей (активной) целевой группы это выглядит примерно так:



Apple iOS

- Закрытая платформа (и меньшая уязвимость)
  - Жесткая политика Apple – не дает рос. разработчикам SDK нижнего уровня (уровня ОС, для работы с “железом”, коммуникациями – порт, SIM)
  - Нет USB, MicroSD, только “закрытый” разъем Apple Dock
  - Jailbreak? Только усугубит проблему безопасности
- Архитектурные ограничения iOS, политика Apple и законодательные ограничения
  - Монолитный код приложений, нет подгружаемых модулей
  - Приложение компилируется вместе с СКЗИ (и содержит СКЗИ…)
  - При распространении приложений через AppStore
    - Приложение не должно содержать криптографию (политика Apple)
    - Получаем распространение нашей криптографии с американского сайта (законодательные ограничения - экспорт криптографии)
  - Единственный путь – “корпоративный AppStore”
    - Приемлем не всегда и не для всех …

Apple iOS - вариант решения

- Использование смарт-карт с сертифицированной российской криптографией и специального карт-ридера

Смарт-карты для Apple iOS - что это дает?

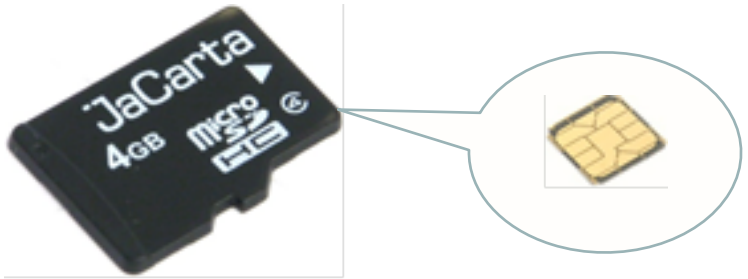
- Соответствие требованиям законодательства
  - ЭП ставится пользователем под документом на его устройстве, с помощью его персонального средства формирования ЭП
- Сокращение сроков выпуска продуктов на рынок
  - Используется уже сертифицированное СКЗИ (средство ЭП)
  - Быстрое встраивание в приложения ЭДО, ДБО и пр. – предоставляем SDK с высокоуровневыми интерфейсами (PKCS#11, PKI-расширение), средства отладки, примеры
    - Поддержка хранения контейнеров КриптоПро CSP
- Упрощается режим эксплуатации
  - Ключи не в устройстве, а на отчуждаемом защищенном носителе – в карте (неизвлекаемые, срок хранения закрытого ключа – 3 года)
- Удобство
  - Одна карта, один ридер – для всех используемых устройств, для всех платформ (ПК, iPad, iPhone)
- Преемственность
  - Карта для входа в домен с ПК, VPN, ЭП и пр.

Мобильные устройства с Android

- Открытая платформа (и потенциально бОльшая уязвимость)
  - Довольно большой “зоопарк”, возможны проблемы совместимости
  - Можно работать с уровнем ОС, с “железом”, с портами
  - Как правило есть USB (но не везде Host), MicroSD
- Средства ЭП – возможные варианты
  1. Карточка Secure MicroSD с интегрированным в нее чипом смарт-карты с сертифицированной криптографией
  2. Смарт-карта с криптографией (+ тот же ридер – один для всех других ПК, планшета, смартфона)
  3. USB-токен с переходником (?)
- Нет единого решения
  - Проблемы “зоопарка”
  - Для карты (ридера) и токена нужен USB-host (есть далеко не везде!)

Secure MicroSD с российской криптографией

Одна карточка Secure MicroSD для всех устройств



SDK для Android - октябрь

Планшет
Телефон

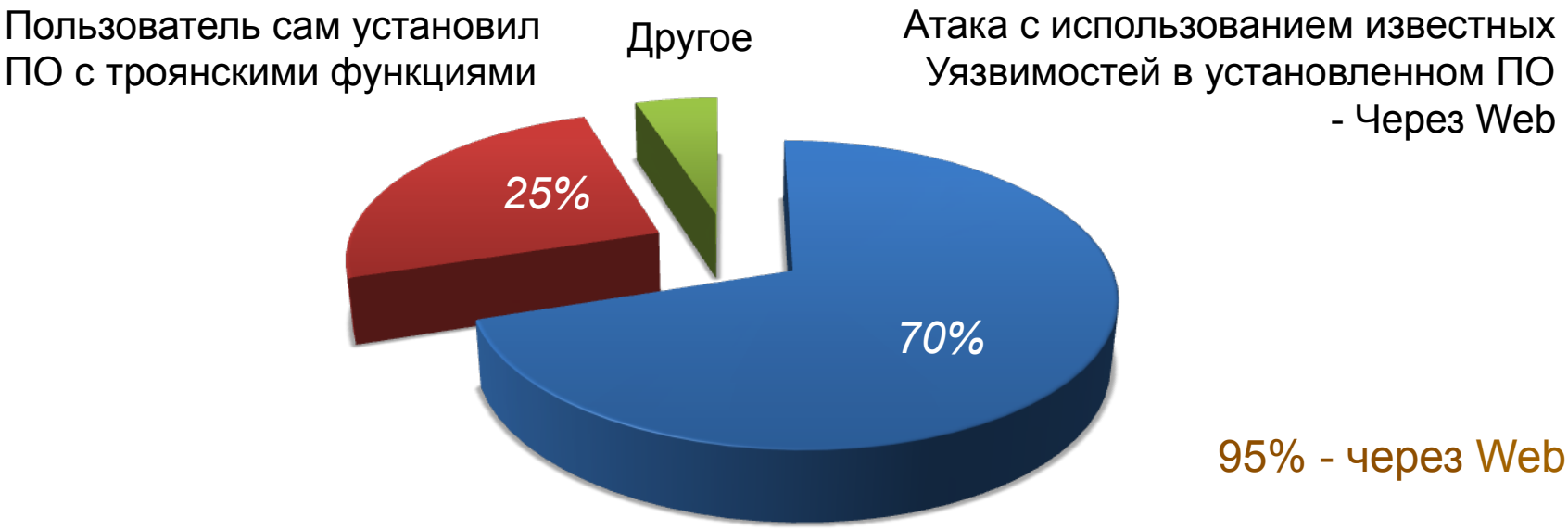
SD-переходник
для ноутбука

USB-переходник
для ноутбука, ПК

Модем с разъемом для
MicroSD – “офис в кармане”

Что с безопасностью применения ЭП на МУ?

- МУ представляются нам менее защищенными чем ПК
  - Живут своей жизнью, сами ставят обновления, пользователи делаю что хотят
- Если смотрим на массовый рынок, то про доверенную среду для ЭП надо забыть
- Что говорят эксперты* – источники инцидентов?

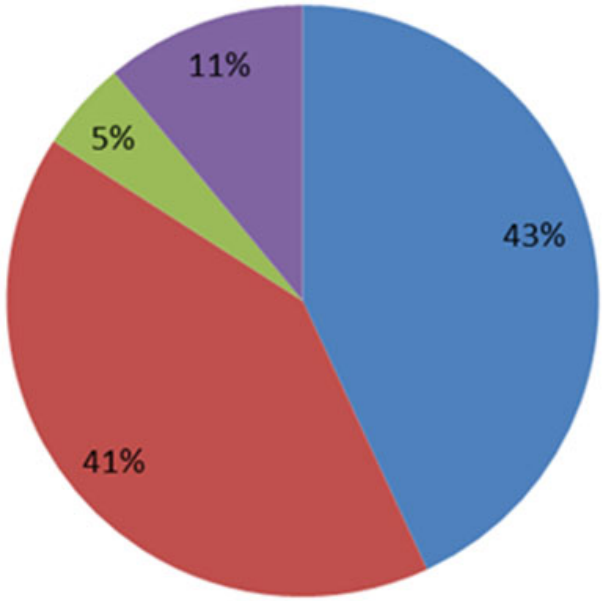


95% - через Web

** - Positive Technology, 2012*

Что с безопасностью применения ЭП на МУ?

- Результаты экспресс-проверки (сотрудники нашей компании, вкл. личные компьютеры, планшеты и смартфоны) – полностью повторяют “ср. среднюю температуру по больнице”:



Связка Браузер-Расширение

- 1-2 уязвимости
- 3-5 уязвимостей
- >5 уязвимостей
- нет уязвимостей - только 11%

На мобильных устройствах (Apple, Android)
уязвимостей не выявлено – пока? / автообновления !!!

На ПК количество браузеров с уязвимостями – 86%
Хуже всего – IE – 62% (из-за механизма патчей)

Что с безопасностью применения ЭП на МУ?

- 95% инцидентов – через эксплуатацию уязвимостей в установленном ПО на клиенте
  - Встроенный сервис проверки в момент подключения и идентификации
  - Передаем на сервер (владельцу системы) данные для фрод-анализа
  - Игнорируя требования обновить ПО или не пользоваться данным устройством, пользователь берет на себя все риски и подписывает согласие своей ЭП
    - При этом понимаем, что мониторинг уязвимостей не панацея, даст эффект при большом количестве пользователей
- **Нужен второй независимый канал**
  - SMS
    - Не гарантированный сервис доставки
    - Возможна подмена (№ абонента, моб. базовая станция)
    - Код подтверждения операции – не ЭП
  - SIM с российской криптографией (ЭП)
    - USSD (обращение по #SIM, передача данных по закрытому каналу)
    - Визуализация значимой информации на экране, подпись ЭП на SIM'ке

Как сделать ЭП действительно массовой?

- G2C, B2C, M2M – нужны полезные и простые сервисы
- Нужны мощные и заинтересованные “двигатели” PKI в массы
  - Надо задействовать существующую инфраструктуру и клиентскую базу **банков** (карты) и **операторов связи** (SIM, MicroSD)
  - Надо привлекать **страховые компании** – это мощный стимулятор
- За счет банков решается вопрос цены и доступности средств ЭП
  - Комбинированная карта – м/н платежная с ЭП “на борту”
  - За эмиссию платежных карт банк все-равно платит…
  - Нужный и понятный сервис – Интернет-банк (с использованием ЭП на карте)
  - Использовать имеющуюся карту с ЭП (и ридер) для других сервисов
  - Примеры: выпуск карт в рамках проекта “Эл. Правительство”

Аладдин РД

Спасибо за Ваше внимание!

Завтрашние технологии
Сегодня!